



Health Industry Cybersecurity Practices (HICP) Quick Start Guide - Small Healthcare Organization



*I'm Part of a Small Practice. Why Should I Even Bother with Cybersecurity?
How can HICP help me become more cyber-prepared?*

As a result of the Cybersecurity Act of 2015, the U.S. Department of Health and Human Services brought together over 150 cyber-experts, clinicians and healthcare administrators to develop the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. The HICP publication provides small healthcare organizations practical, cost-effective practices that lessen cybersecurity risks by improving your staff's "cyber hygiene."

Cybersecurity threats to small practices are real. Hackers of all types (nation-state actors, cyber criminals, hacktivists, etc.) have found numerous ways to make money from illegally obtained healthcare data; they have increasingly targeted small healthcare organizations—they're not just going after the "big guys."

Individual practitioners or small practices that succumb to an attack can lose their reputation and trust in their communities—leading to financial consequences. Everyone is a patient, and your community needs your organization to provide healthcare! With this in mind, your organization's IT professionals or third-party service provider should perform practical and cost-effective cybersecurity practices. These practices may reduce the risk of a cyberattack that could hurt your business and your community.

Understand How Adopting HICP Can Benefit Your Organization



WHAT IS HICP?

The HICP publication identifies five current cybersecurity threats and provides ten practices that can be used to mitigate them. It's comprised of a common set of cost-effective best practices based on widely accepted and used frameworks, standards, methodologies, processes, and procedures vetted by healthcare and security professionals.



WHO DOES HICP BENEFIT?

Small Practices like yours! HICP is designed to strengthen the cybersecurity posture of the healthcare industry, and help small practices prioritize what is important for their own protection. By using HICP, small practices can do their part to support the national healthcare industry's cyber preparedness.



WHAT ARE THE FIVE THREATS?

The five current threats detailed in the HICP main document are: E-Mail Phishing Attacks; Ransomware Attacks; Loss or Theft of Equipment or Data; Insider, Accidental, or Intentional Data Loss; and Attacks Against Connected Medical Devices.



WHAT ARE THE TEN BEST PRACTICES?

HICP identifies ten best practices to mitigate the current threats: E-Mail Protection Systems; Endpoint Protection Systems; Access Management; Data Protection and Loss Prevention; Asset Management; Network Management; Vulnerability Management; Incident Response; Medical Device Security; and Cybersecurity Policies.

How is the HICP Publication Organized?

The HICP Publication includes a main document, two technical volumes, and a Resources and Templates Volume:

- The [Main Document \(MD\)](#) discusses the current cybersecurity threats facing the healthcare industry.
- [Technical Volume 1 \(TV1\)](#) discusses 10 Cybersecurity Practices for small healthcare organizations.
- [Technical Volume 2 \(TV2\)](#) discusses 10 Cybersecurity Practices for medium-sized and large healthcare organizations.
- The [Resources and Templates Volume](#) provides additional resources, templates, and supplementary materials.

How Can I Use this Quick Start Guide?

The HICP Publication encourages good cyber hygiene across your small practice. After reading this quick start guide, you will understand which HICP documents are most applicable to each role at your organization and what to do next. Look up your role in the matrix below so you know what you should read—and what you should delegate. Leadership and management are in the first column, technology professionals in the second column, staff users including practitioners, nurses, administrative professionals, and any network user are in the third column.



What's your role	Leadership & Management	Technology Professionals	Staff/Users (ANY network user)
What part of HICP you should read	MD – pages 5-10 MD – page 28 T1 – pages 3-4	MD – page 11 MD – page 28 T1 – Entire Document	MD – pages 15–26
What part of HICP you should pass along and to whom	To Your Organization's Technology Professionals: MD – page 11 MD – page 28 T1 – Entire Document	To Your Organization's Leadership & Management: MD – pages 5-10 MD – page 28 T1 – pages 3-4	To Your Organization's Leadership & Management: MD – pages 5-10 MD – page 28 T1 – pages 3-4
	To Your Organization's Staff/Users: MD – pages 15–26	To Your Organization's Staff/Users: MD – pages 15–26	To Your Organization's Technology Professionals/ Third Party Service Provider: MD – page 11 MD – page 28 T1 – Entire Document